U.S. Department of the Interior
Office of Inspector General

AUDIT REPORT

GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE

REPORT NO. 98-I-336
MARCH 1998

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

MAR 2 4 1998

MEMORANDUM

TO: The Secretary

FROM: Robert J. Williams Robert J. Williams
Acting Inspector General

SUBJECT SUMMARY: Final Audit Report for Your Information - "General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service" (No. 98-I-336)

Attached for your information is a copy of the subject final audit report. The objective of our audit was to evaluate the adequacy of the general controls over the Minerals Management Service Royalty Management Program's automated information system in the areas of security program development, physical and logical access, software development and change management, separation of duties, system software, and service continuity.

We found that the Royalty Management Program had established general controls over its automated information system; however, except for the controls over physical access to the automated information system, we concluded that the general controls were not adequate in the six major areas reviewed. Specifically, the Program did not identify and address all risks affecting proprietary and financial data in the automated information system, have adequate security-related personnel policies and procedures, and have security awareness statements on file for all employees who used the automated information system; have adequate logical access controls in the areas of resource classification, default settings, commercial off-the-shelf software access controls, access levels granted to users, and numbers of allowed log-in attempts; have controls to ensure that client/server application software changes were authorized, approved, and tested before being moved into production; separate the duties of the client/server application programmers from the duties of the users and separate the duties of client/server security administrators from reviewers; use mainframe security software that was supported by the vendor and use available mainframe computer system audit tools to ensure integrity over system processing and data; and include local area networks and personal computers which maintain proprietary and financial data in the Program's disaster recovery plans. We made 24 recommendations to improve the general controls over the Program's automated information system.

Based on the response to the draft report from the Director, Minerals Management Service, we deleted one recommendation and revised one recommendation. Also, based on the response, we considered 1 recommendation resolved and implemented and 12 recommendations unresolved, and we requested additional information for 10 recommendations.

If you have any questions concerning this matter, please contact me at (202) 208-5745.

Attachment

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

MAR 23 1998

AUDIT REPORT

Memorandum

To: Director, Minerals Management Service

From: Robert J. Williams Robert J. Williams
Acting Inspector General

Subject: Audit Report on General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service (No. 98-I-336)

INTRODUCTION

This report presents the results of our audit of the general controls over the automated information system at the Minerals Management Service's Royalty Management Program. We performed this audit to support our audit of the Service's financial statements, which is required by the Chief Financial Officers Act. The objective of this audit was to evaluate the adequacy of the general controls over the Program's automated information system in the areas of security program development, physical and logical access, software development and change management, separation of duties, system software, and service continuity.[1]

BACKGROUND

The Minerals Management Service's Royalty Management Program is responsible for collecting and disbursing revenues of about $4 billion annually that are generated from leasing Federal and Indian lands and for collecting royalties for minerals extracted from leased lands. To aid in accomplishing its mission objectives and meeting its financial reporting requirements, the Program uses an automated information system that includes a mainframe computer, a minicomputer, and personal computers and servers which support local area networks for each Program division, a wide area network, and an enterprisewide

[1] Logical access refers to controls that provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make. (An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, National Institute of Standards and Technology.)

network.[2] For collecting rents and royalties, the Program primarily uses the mainframe computer. For disbursing rents and royalties, verifying collections, and reporting financial information, the Program uses all of the components of its automated information system.

The Program's mainframe computer, minicomputer, and some of the personal computers and servers are located in three buildings at the Denver Federal Center, in Denver, Colorado. The Program also has personal computers and servers located in leased buildings in Golden, Colorado, and at Program division offices in Dallas and Houston, Texas.

Since 1992, Program management has been planning, developing, and moving to a "client/server" processing environment.[3] In a client/server environment, data are more difficult to protect. Specifically, the data are stored and processed in multiple locations, and the data must travel through telecommunication systems between the clients and the servers where the data are inherently susceptible to being released to unauthorized outside parties, lost, or damaged. Additionally, the Program's data are "proprietary"; therefore, if access to the data is denied or if the data are inappropriately released, lost, or damaged, the Program, suppliers of the data, or others having an interest in the data could be adversely impacted.

The Program's automated information system was operated and maintained by the contractor American Management Systems Operations Corporation. The contract with the Corporation requires the Corporation to: (1) maintain system software; (2) maintain and develop application software; and (3) maintain other software, such as teleprocessing and general utilities.

Overall system security policies for the Program are established by the Installation Automated Information System Security Officer, within the Program's Systems Management Division. System security administration for the mainframe computer, the minicomputer, the wide area network, and the enterprisewide network is the responsibility of the Corporation. Security administration for the Program's local area networks is the responsibility of each of the Program's seven divisions, which consist of the Accounting and Reports Division, the Royalty Valuation Division, the Systems Management Division, the State and Indian Compliance Division, and the Compliance Divisions at Dallas and Houston and Lakewood, Colorado.

[2] Servers are computers that provide services to client computers on a network. Local area networks are communication networks located in a small geographical area which connect many computerized input/output devices, generally server computers, client computers, and peripheral hardware such as printers, through low-cost communication mediums. These networks typically do not use common carrier circuits, such as U.S. West, and their circuits do not cross public thoroughfares or property owned by others. Wide area networks span large geographical areas and typically use circuits provided by common carriers. Enterprisewide networks are networks that result when all the networks in a single organization are connected together. (Jerry Fitzgerald and Alan Dennis, Business Data Communications and Networking, 5th edition, John Wiley & Sons, Inc., 1996, pps. 249, 522, 529, 542, and 549.)

[3] A "client/server" processing environment is a computerized architecture in which one or more "computers called servers manage shared resources and provide access to those shared resources as a service to their clients," which are personal computers. (David Vaskevitch, Client /Server Strategies, a Survival Guide for Corporate Reengineering, IDG Books Worldwide, Inc., San Mateo, California, 1993, page 96.)

SCOPE OF AUDIT

To accomplish our objective, we reviewed the general controls that were in place during January through June 1997. Specifically, we reviewed the controls in six major areas: security program development; logical and physical access; software development and change management; separation of duties; system software; and service continuity. We interviewed Program and contractor personnel, reviewed systems documentation, observed and became familiar with computer center operations and network components, analyzed system security, and evaluated service continuity procedures and testing. In addition, we reviewed procedures to maintain system and application software for the mainframe computer, the local area networks, the wide area network, and the enterprisewide network. Because our review was limited to evaluating the adequacy of general controls over the automated information system, we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information system general controls. While our objective was to review the general controls of the automated information system, the primary emphasis was on the servers that supported data processed and maintained on the local area, wide area, and enterprisewide networks.

Our audit, which was conducted during December 1996 through August 1997 at the Program's facilities in Denver and Golden, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the internal controls that could adversely affect the Program's automated information system. The control weaknesses that we found are summarized in the Results of Audit section and discussed in detail in Appendix 1 to this report. If implemented, our recommendations should improve the internal controls in the areas reviewed. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the objective and scope of this audit: However, in July 1997, the Office of Inspector General issued the report "Royalty Management Program's Automated Information Systems, Minerals Management Service" (No. 97-I-1042), which identified weaknesses in mainframe application software development and change management. During our current audit, we noted that Program management had agreed with the seven recommendations made in our prior audit report and that two of the seven recommendations had been implemented. One of the implemented recommendations and three of the recommendations that were resolved but not implemented affected the change request process (change management), which is discussed in the scope of this audit. We further noted that implementation of the three recommendations was delayed because of the priority of implementing the changes mandated by the Federal Oil and Gas Royalty Simplification and Fairness Act of 1996.

RESULTS OF AUDIT

The Royalty Management Program had established general controls over its automated information system; however, except for the controls over physical access to the automated information system, we concluded that the general controls were not adequate in the six major areas reviewed. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies.[4] Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls over the sensitive information is adequate. Further, the Department of the Interior and the Program have issued policies and procedures to implement general controls to protect sensitive data in automated information systems. The controls were not adequate because Program management had not established necessary policies and procedures, had not assigned responsibilities for ensuring that policies and procedures were developed and followed, and had not held officials accountable for noncompliance with the established controls. The lack of adequate controls increased the risk of (1) unauthorized access and modifications to and disclosure of Program data, (2) theft or destruction of Program software and sensitive information, and (3) loss of critical Program systems and functions in the event of a disaster or system failure.

Overall, we identified 13 weaknesses and made 23 recommendations for improving the general controls over the Program's automated information system. A summary of the weaknesses noted in the six major areas is provided in the following paragraphs, and specific details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program Development

We found weaknesses in the automated information system security program. Specifically, Program management did not identify and address all risks affecting proprietary and financial data in the automated information system, did not have adequate security-related personnel policies and procedures, and did not have security awareness statements on file for all employees who used the automated information system. As a result, there was an increased risk that sensitive data may be impaired or compromised by individuals and that data may be inadvertently disclosed or destroyed or erroneously modified. We made seven recommendations to address these weaknesses.

[4] The Computer Security Act defines "sensitive" data as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act."

Access Controls

We found weaknesses in logical access controls over the Program's automated information system. These weaknesses were in the areas of resource classification, default settings, commercial off-the-shelf software access controls, access levels granted to users, and numbers of allowed log-in attempts. As a result, there was an increased risk that sensitive data maintained on the automated information system were vulnerable to unauthorized access, manipulation, and disclosure. We made eight recommendations to address these weaknesses.

Software Development and Change Management

We found that the controls over changes to client/server application software were not adequate. Specifically, Program management did not have controls to ensure that client/server application software changes were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that the most critical client/server application software changes were not made and that client/server applications would not perform as intended. We made one recommendation to address this weakness.

Separation of Duties

We found that Program management did not separate the duties of the client/server application programmers from the duties of the users and did not separate the duties of client/server security administrators from reviewers. As a result, there was an increased risk that accidental or intentional actions by programmers could threaten the integrity of the Program's data and disrupt system processing and that inappropriate actions by security administrators would not be detected or detected timely. We made two recommendations to address these weaknesses.

System Software Controls

We found that the controls over system software were not adequate in detecting and determining inappropriate use. Specifically, the security software in use for the mainframe computer was no longer supported by the vendor, and available mainframe computer system audit tools to ensure integrity over system processing and data were not used. As a result, there was an increased risk that programs and data files would not be protected from unauthorized access and that inappropriate mainframe computer system initialization and processing would not be recorded and identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities may not be detected or detected timely and that the responsible individual or individuals may not be held accountable for the inappropriate action. We made four recommendations to address these weaknesses.

Service Continuity

We found that local area networks and personal computers used by the Program's divisions which maintain proprietary and financial data were not included in the Program's disaster recovery plans. As a result, there was an increased risk that critical systems may not be recovered in the event of a disaster or system failure. We made one recommendation to address this weakness.

Minerals Management Service Response and Office of Inspector General Reply

In the January 21, 1998, response (Appendix 2) from the Director, Minerals Management Service, to our draft report, the Service stated that of the report's 24 recommendations, it "agree[d]" with 11 recommendations, "partially agree[d]" with 2 recommendations, and "disagree[d]" with 11 recommendations. Based on the response, we deleted one recommendation (No. F.3) and revised one recommendation (No. I.1) in the draft report. Also based on the response, we consider 1 recommendation resolved and implemented and 12 recommendations unresolved, and we request additional information for 10 recommendations. The status of each recommendation is in Appendix 3, and the Service's responses to the recommendations and our comments are presented within each finding.

Additional Comments on Audit Report

The Service said that it "disagree[d]" with the overall "implicit conclusion" that the Royalty Management Program's automated information system was not in compliance with Office of Management and Budget Circular A-130 and that it believes that it is in "substantial compliance with the spirit and intent" of the Circular. Further, the Service stated that the audit report "does not actually deal with the overall or general controls" because we did not review redundant and compensating controls. In addition, the Service stated that "recurring management control reviews have addressed such manual controls and generally found they were working effectively or prompted corrective actions to resolve minor control deficiencies." Further, the Service stated that "audits performed under the Chief Financial Officers Act of 1990 have covered these controls, and each report concluded that our financial information was reliable."

The criteria we used included not only Office of Management and Budget Circular A-130 but also standards and guidelines referenced in the Circular from the Department of Commerce (National Institute of Standards and Technology), the General Services Administration, and the Office of Personnel Management and policies and procedures of the Department and the Program. Since the controls cited in and referenced by Appendix III of Circular A-130 are "a minimum set of controls" to be included in an agency's automated information security program, we believe that any deviation from these minimum controls would indicate that an agency's automated information system security program does not reduce risk to an acceptable level and ensure that an agency is in compliance with the Circular. However, since our review identified weaknesses in the general controls over the automated information system in the areas of security program development, access controls, software development and change management, separation of duties, system software controls, and service continuity, we do not believe that the Service's "substantial compliance" with the minimum controls set forth in the Circular was adequate to address the potential risks identified by our review.

While we stated that we did not evaluate the effectiveness of manual control procedures which may have operated as compensating controls in the scope section of the report, the audit staff did evaluate the general controls that were defined in the Program's policies and procedures. Because redundant or compensating controls were not cited by the Program in its policies and procedures as the primary controls used to ensure the integrity, confidentiality, and availability of Program information, these controls were not evaluated.

During the audit, we reviewed an Automated Information Systems Review that the Service performed in fiscal year 1996 which concentrated on the Program's change management controls over applications in the mainframe environment. The Service's review identified weaknesses concerning application testing and documentation that we also cited in the Prior Audit section of this report. Further, we found similar weaknesses in software development and change management controls in the client/server environment (see Finding I in Appendix 1.)

While we are not questioning that the financial statements were presented fairly, we found, as a result of our evaluation, inadequacies in the Program's general controls over the automated information system in the areas of security program development, access controls, software development and change management, separation of duties, system software controls, and service continuity. These weaknesses, identified with the general controls, will result in our having to raise the overall level of risk of possible loss associated with the internal control structure of the Royalty Management Program in future financial statement audits.

Regarding system security, we agree that system security controls implemented should be measured against costs and risks. However, the Program did not provide evidence that such a measurement study was performed. Further, our findings identified breakdowns in existing controls cited in the Program's policies and procedures. While no system is completely free of errors, an adequate security program would provide a foundation for the Service to determine what controls were operating effectively and the level of risk that the Service is mitigating with these controls.

We disagree that the Program is being held to "unattainable standards" because the standards we used were those cited in Appendix III of Circular A-130 as "the minimum set of controls" to be included in an agency's automated information security program. In addition, in our evaluation of the Program's general controls as defined in its policies and procedures, we found that the controls were not operating effectively.

We disagree with the Service's statement that our findings did not demonstrate a "single negative impact" because the impact of these inadequacies taken as a whole indicates that there is no assurance that the overall risk to the Program was at an acceptable level.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by April 17, 1998. The response should provide the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Minerals Management Service personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

A. Risk Assessments

Condition: Risk assessments of the Royalty Management Program's automated information system did not identify and address all risks affecting proprietary and financial data in the automated information system or correctly assess some of the risk elements. For example, we found that Program management did not:

- Identify and address the impact that (1) converting to the year 2000 would have on application processing, (2) using system security software which is no longer supported by the vendor could have on operations, and (3) having royalty and financial information on local area network applications and personal computer databases could have on operations.

- Correctly assess the risk for the "Geopolitical" and "External Directives" elements, which were assessed as low risk. Significant geopolitical and external directives, such as the possible abolishment of the Program and the enactment of the Federal Oil and Gas Royalty Simplification and Fairness Act, have impacted the Program during the past 2 years. We believe that the level of risk associated with these elements was such that it increased the potential for lowering employee morale and thus increased the risk of sabotage or breach of other physical security measures, as well as the possibility of data errors and omissions that affect data and system integrity.

Criteria: Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," states that adequate security "includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls." The Circular further states that, although formal risk analyses need not be performed, "the need to determine adequate security will require that a risk-based approach be used." According to the Circular, "This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" provides guidance on computer security risk management. The NIST Handbook specifically addresses the

SECURITY PROGRAM

selection of safeguards to mitigate risk and the acceptance of residual risk. In addition, Program policy requires that local area network administrators participate in the risk assessment process.

Cause: Program management did not ensure that risk assessments were performed in accordance with risk management guidelines. Specifically, the assessments did not address (1) all risks associated with its automated information system, (2) the selection of safeguards to mitigate risks, and (3) the acceptance of residual risk. In addition, Program management did not effectively communicate the responsibility of local area network administrators to participate in risk assessments and had not adequately addressed that local area network applications and personal computer databases should be included in the Program's security program.

Effect: Without identifying all significant threats and vulnerabilities to the automated information system, Program management was unable to determine the most appropriate measures needed to protect against threats or reduce the vulnerabilities. Further, without including the Program's local area network applications and personal computer databases as part of the risk assessments, there was little assurance that all threats and vulnerabilities were identified and considered when Program security policies and plans were developed. Therefore, there was an increased risk that critical Program resources would not be adequately protected and that expensive controls would be implemented for resources that did not require significant protection.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Ensure that risk assessments are conducted in accordance with guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.

2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.

3. Determine the risks associated with local area network applications and personal computer databases which contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.

SECURITY PROGRAM

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendation 3 and that it reconsider its responses to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that it "plans to enhance and better document" its risk assessment process. The Service further stated that it believed its "previous assessments were in accordance with guidelines" because of the "rapidly changing computing and communication environment."

Office of Inspector General Reply. We disagree that "previous assessments were in accordance with guidelines." Office of Management and Budget Circular A-130, Appendix III, and referenced standards and guidelines of the National Institute of Standards and Technology state that "risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk." Since the Service did not address a number of significant conditions/issues that affect risks to the Program's automated information system, identify the risks associated with these conditions, or identify the controls in place to reduce the risks to an acceptable level, we believe that the Program's risk assessment process was not in accordance with the guidelines. Additionally, Appendix III of Circular A-130 was revised so that Federal computer security programs could better respond to the rapidly changing technological environment. Although the Service disagreed with the recommendation, we believe that its action to enhance and document its risk assessment process is indicative of its intent to comply with the recommendation. However, we request that the Service clarify its intent (see Appendix 3).

Recommendation 2. Nonconcurrence.

Service Response. The Service stated that policies "define the LAN [local area network] administrators' role in contingency planning and security," and it provided additional information to support its position.

Office of Inspector General Reply. While the additional information did address the administrators' role in contingency planning and security, it did not address the recommendation. The "RMP Automated Information Systems Security Manual" states that administrators should participate in the risk assessment process. During our audit, we found that the administrators were not always aware of their responsibilities to identify risks and implement controls that would mitigate risks and that the administrators' individual position descriptions did not always address these responsibilities.

Additional Comments on Finding

The Service stated that it believes that we did not apply risk assessment criteria appropriately because "Circular A-130 states '*the Appendix no longer requires the preparation of formal risk analyses*' and that risk assessments '*can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments.*'"

We agree that formal risk analyses are not required and that risk assessments can be formal or informal. However, we found that the Program's analyses were not based on risk-based management as described by Appendix III of Circular A-130 and referenced standards and guidelines of other Federal executive branch agencies and the Departmental Manual (375 DM 19). According to the NIST Handbook, risk-based management "is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk." In its response, the Service provided additional information related to each of the examples in this finding. However, the additional information provided did not indicate that the Program used risk-based management in developing its controls.

SECURITY PROGRAM

B. Security-Related Personnel Policies and Procedures

Condition: The Program's security-related personnel policies and procedures were not adequate to ensure system integrity. Specifically, we found that:

- Contractor employees received the same type of background check and security clearance regardless of their duties and the risk associated with the computer-related work they performed. Thus, contractor employees, such as system programmers and computer operators, who could bypass technical and operational controls, received the same security clearance as administrative assistants.

- Computer-related work was not technically reviewed by contractor or Program personnel whose position sensitivity was greater than that of the position sensitivity of individuals performing the work.

- Contractor employees did not always submit requests for background checks for security clearances. Further, the requests that were submitted for background checks were not submitted within the time frames specified in the contract. An average of 175 calendar days elapsed, instead of the 2 weeks stipulated in the contract, between the dates the employees were hired and the dates the requests were received by the Minerals Management Service's Security Officer in Personnel for forwarding to the Office of Personnel Management. The Office of Personnel Management performed background checks for the same employees in an average of 84 days, and the Minerals Management Service approved the security clearances in an average of 22 days. Thus, most of the delay in the security clearance process was attributable to contractor and Program personnel.

- Systems Management Division employees did not have documentation to support that appropriate background checks for security clearances and required periodic followup background checks had been performed.

Criteria: The Departmental Manual (441 DM) specifies that position sensitivity should be based upon risk factors such as degree of public trust, fiduciary responsibilities, importance to program, program authority level, and supervision received. In addition, the Manual requires consideration of automated data processing (ADP) factors, such as the level of responsibility and technical review of work, for incumbents who are responsible for planning, directing, and implementing computer security; planning, directing, implementing, operating, and maintaining computer systems; and accessing or

SECURITY PROGRAM

processing automated information records systems that contain proprietary data. Further, work is to be technically reviewed by individuals filling ADP "critical-sensitive" positions when individuals filling ADP "noncritical-sensitive" positions perform computer work such as directing, planning, designing, operating, and maintaining a computer system to ensure system integrity. In addition, the terms of the contract require that the "assistant manager" positions' sensitivity level be ADP "critical-sensitive," that background check requests be submitted to the Service within 2 weeks after an employee's hire date, and that the employees be in probationary status until the background checks are completed and the security clearances are approved.

Cause: The Systems Management Division staff and the contractor staff who were responsible for technical reviews of the work were not in positions classified as ADP "critical-sensitive." Additionally, Program contracting personnel did not ensure that contractor personnel (1) submitted requests for background checks and (2) remained in probationary status and did not perform critical computer work until background checks were completed and security clearances were approved. Further, personnel or security files did not reflect that appropriate background checks or that required periodic followup background checks were performed.

Effect: As a result, there was an increased risk that employees would perform critical automated information system operations and maintenance work without appropriate oversight or adequate assurance that their backgrounds would warrant such trust.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Evaluate Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity levels are greater than the position sensitivity levels of the employees who are performing the work.

2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.

SECURITY PROGRAM

3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic followup background checks are performed as required.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendations 1 and 2 and that it reconsider its response to Recommendation 3, which is unresolved (see Appendix 3).

Recommendation 1. Partially concur.

Service Response. The Service stated it planned to "reevaluate the position sensitivity level for the senior personnel in charge of the contractor activity to determine if those position[s] should be classified at a higher level. In accordance with Departmental criteria, most ADP [automated data processing] staff are designated noncritical sensitive. We doubt it was the OIG's [Office of Inspector General] intention to imply that *all* work must be reviewed by persons at a higher sensitivity level; however, this would be impossible in a multiple level organization because there are only two sensitivity levels from which to choose, i.e., 'noncritical-sensitive' and critical-sensitive.'"

Office of Inspector General Reply. The Departmental Manual identifies four sensitivity levels. Further, although the Service indicated that some staff would have the next higher security level of "critical-sensitive" to perform technical reviews, we found that only one ADP staff position was classified as "critical-sensitive" and that the position was not responsible for performing technical reviews. Although the Service only partially concurred with the recommendation, we believe that the action to reevaluate position sensitivity levels is indicative of its intent to comply with the recommendation.

Recommendation 2. Partially concur.

Service Response. The Service said that it agreed that controls were needed to ensure that the contractor submitted requests for background checks in a timely manner. The Service further stated that the contractor had been "directed" and had "begun to track and is accountable for the status of its submission of these requests." The Service also said that it agreed that contractor employees awaiting clearances should be in "probationary status" but that having the employees not performing their assigned duties would be "unacceptably costly." According to the Service, it was "exploring alternatives" with the contractor such as having the contractor "perform a preliminary 'criminal and credit check' which is quick and inexpensive."

SECURITY PROGRAM

Office of Inspector General Reply. Preliminary investigations would be a suitable alternative to prohibiting contractor employees from performing their assigned duties before the background clearances have been accomplished. Although the Service only partially concurred with the recommendation, we believe that its action to evaluate alternatives such as preliminary investigations is indicative of its intent to comply with this recommendation.

Recommendation 3. Nonconcurrence.

Service Response. The Service stated that controls are "in place to ensure that personnel or security files accurately reflect background checks." The Service further stated that its Office of Administration and Budget "maintains documentation and a tracking system" on all security clearances and background checks of its employees and contractors. The Service stated that it disagreed with our statement that followup background checks are required, stating that it is in compliance with Department of the Interior guidance which states that followup checks "are authorized *only* for national security positions and not for public trust positions."

Office of Inspector General Reply. The Office of Administration and Budget's documentation and tracking system, while serving as part of the control, did not ensure that personnel or security files accurately reflected that background checks were requested and documented in the "official personnel files" of the employees. Additionally, the Departmental guidance included by the Service was dated 1993; however, the Code of Federal Regulations (5 CFR 1), dated 1997, states that followup background checks are required of employees in positions that are for national security and other positions considered to be "high risk." The Office's Security Officer verified that the Program has employees in "high risk" positions, such as the Chief, Systems Management Division; the Installation Security Officer; the Contractor's Project Manager; and supervisors within the Systems Management Division. As such, employees in these positions would be required to have followup background checks.

SECURITY PROGRAM

C. Security Awareness Statements

Condition: We found that automated information system users did not have security awareness statements on file acknowledging the employees' acceptance of their responsibilities to safeguard the Program's proprietary data and assets.

Criteria: The Department's "Automated Information Systems Security Handbook" requires employees who use sensitive automated information system resources to sign statements acknowledging their responsibilities for the security of the resources. Additionally, the "RMP [Royalty Management Program] Automated Information Systems Security Manual" requires that employees sign a Minerals Management Service Security Statement, which acknowledges their responsibilities to safeguard Program-sensitive data and assets, and requires the Installation Automated Information System Security Officer (Installation Security Officer) to verify that security awareness statements are signed by the employees before their system access requests are approved.

Cause: Program management did not ensure that its employees signed security awareness statements. In addition, the Installation Security Officer did not ensure that security statements were on file before the Installation Security Officer approved access to the automated information system.

Effect: As a result, employees may not be aware of their responsibilities to safeguard automated information system data and assets and thus inadvertently disclose sensitive information.

Recommendation:

We recommend that the Director, Minerals Management Service, establish controls to enforce Program policy which requires employees to sign security awareness statements before access to system resources is approved by the Installation Automated Information System Security Officer.

SECURITY PROGRAM

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its response to the recommendation, which is unresolved (see Appendix 3).

The Service stated that while its own test sample confirmed that users have appropriate access to the Program's systems, it "concur[s] that [its] filing system for access approvals needed improvement." The Service further stated that all statements are "now consistently filed and reconciled by the ADP security officer."

The Service agreed with the recommendation and said that it was implemented. However, while the security awareness statements referred to in the finding provide evidence that users accepted their responsibility to safeguard the Program's proprietary data and assets, these statements do not support the appropriateness of access to Program systems. Without familiarity with the methodology employed in the Service's test, such as sample selection and test performance, we must rely on the tests performed using statistical sampling software and generally accepted Government auditing standards followed by the audit staff. Further, the Service stated, in its response to Recommendation D.2, that "all MMS [Minerals Management Service] employees are granted access to view royalty, production, and reference data." Accordingly, if the Service's tests did not include all Service employees, there is no assurance that all statements have been filed and reconciled. Therefore, we consider this recommendation unresolved and request that the Service reconsider its response to the recommendation (see Appendix 3).

ACCESS CONTROLS

D. Resource Classifications

Condition: The Program's computer resources (data files, application programs, and computer-related facilities and equipment) were not classified appropriately to determine the levels of access controls that should be implemented over the resources. For example, no "major application"[1] was identified in the Program's annual security plan, even though the applications and data files were "proprietary" and critical to the Program in accomplishing its mission and reporting financial information. Further, access controls over sensitive data on the servers used by the Program's divisions were not as stringent as the access controls over sensitive data on the mainframe.

Criteria: Office of Management and Budget Circular A-130, Appendix III, directs agencies to assume that all major systems contain some sensitive information that needs to be protected but to focus extra security controls on a limited number of particularly high-risk or major applications. According to the NIST Handbook, "Security levels, costs, measures, practices, and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability, and extent of potential harm." Further, the determinations should flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or failing to protect the integrity of data supporting critical transactions or decisions. Accordingly, Program policy requires that users be given access only to the resources needed to perform their assigned duties.

Cause: Program management had not identified the resources that needed significant protection. Further, Program management did not require application owners who are responsible for approving user access levels to the applications to classify their resources based on the level of sensitivity of the information contained in their applications.

Effect: As a result, there was an increased risk that resources were not adequately protected from unauthorized access and disclosure and therefore were subject to either accidental or intentional changes to computer operations and data.

[1] Office of Management and Budget Circular A-130, Appendix III, identifies a "major application" as an "application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." The Appendix further states that "certain applications, because of the information in them, however, require special management oversight and should be treated as major."

Conversely, the level of protection provided for low-risk resources may be in excess of that required. Furthermore, Program management did not have a reliable basis for making critical decisions regarding security safeguards for its sensitive applications.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.

2. Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its response to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service said that it believed that its "current classifications are appropriate." The Service further stated that its mainframe systems "receive heightened security because they are more mission critical, not because they are more sensitive" and that these systems "must be protected more strenuously to ensure the integrity of the official records." The Service also stated: "A more moderate level of protection is necessary for proprietary information than for mission critical information. The umbrella protection mechanism for all types of proprietary information is physical controls coupled with employee training."

Office of Inspector General Reply. We disagree that the Service's current classifications are appropriate. In its response to Recommendation M.1, the Service indicated that the Program had not identified all "mission critical" systems. Further, in our opinion, mission critical systems resided on personal computers and local area networks that supported the Program's mission to accurately and timely disburse rents, bonuses, and royalty revenues to the U.S. Treasury, the states, and the Indian tribes, as well as financial transactions and external reporting. Additionally, the Service stated that the umbrella protection over its proprietary data, which do not reside on the mainframe computer, is

ACCESS CONTROLS

limited to "physical controls" and "employee training." However, these controls do not meet the minimum controls required for Federal automated information resources. The purpose of resource classification is to provide a basis for determining the controls necessary to ensure appropriate implementation of risk-based management, as required by Office of Management and Budget Circular A-130, Appendix III.

Recommendation 2. Nonconcurrence.

Service Response. The Service said that it believes that its "existing access controls over resources already meet the intent of this recommendation." The Service further stated that all of its employees "are granted access to view royalty, production, and reference data. Since most of this data is proprietary, employees are trained in its proper use and must sign statements acknowledging their responsibility to protect it. State and Tribal employees have access to such data within their jurisdictions only. The ability to add or change data is limited to those employees who require that access to perform their jobs."

Office of Inspector General Reply. We disagree that the Service's existing access controls meet the intent of the recommendation. By its response, we inferred that the Service had not complied with the personnel control of "least privilege" required by Appendix III of Circular A-130 and the "RMP Automated Information Systems Security Manual." The Circular defines least privilege as "the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read [which means to view], write, execute, delete) to the minimum necessary to perform" an employee's job. Further, the Program's Manual states, "[P]rivileges granted to users are only those privileges that are absolutely necessary for job performance." In addition, Appendix III of Circular A-130 and the Departmental Manual (375 DM 19) state that the "greatest threat" to most computer systems comes from authorized users. However, as stated by the Service, "All [Service] employees are granted access to view royalty, production, and reference data." Therefore, we believe that allowing all Service employees to have access to view Program data indicates that access controls were not implemented commensurate with the level of risk and sensitivity of each resource. Further, as cited in Findings E, F, and G in this report, controls over access were inadequate; therefore, we believe that the Service's current access controls over resources do not meet the intent of the recommendation.

ACCESS CONTROLS

E. Default Settings Provided With Commercial Off-the-Shelf Software

Condition: Default settings provided with commercial off-the-shelf software were not removed after the software was installed and implemented. For example, we found that the default user identification (ID) and associated default password had not been removed when Program management upgraded to the latest version of the Integrated Data Management System (IDMS).[2] The default user ID provides users with administrative privileges to establish and remove users and to access all mainframe computer resources.

Criteria: The "RMP Automated Information Systems Security Manual" requires that default user IDs and passwords be removed once commercial off-the-shelf software is implemented.

Cause: Rather than deleting the default user ID and password, Program management relied on the mainframe security software to protect against unauthorized access.

Effect: As a result, there was an increased risk that the automated information system could be accessed by unauthorized users.

Recommendation:

We recommend that the Director, Minerals Management Service, implement controls to enforce Program policy that default user IDs and passwords are to be removed from the automated information system when commercial off-the-shelf software is implemented.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with the recommendation. However, the Service needs to provide additional information for the recommendation (see Appendix 3).

Additional Comments on Finding

Even though the Service agreed with this recommendation, it stated that our conclusion was incorrect that "the use of this default ID allows access to all mainframe computer resources" because "the security architecture prevented" the misuse of resources. The security

[2] Integrated Data Management System (IDMS) is a licensed product of Computer Associates International, Inc., which manages database applications that reside on mainframe computers.

ACCESS CONTROLS

architecture requires that a user who wants to access the mainframe have a "valid RACF logon password" and a "user ID defined to the data dictionary." We disagree that the security architecture prevented the misuse of resources. Vendor documentation states that the default ID can be used to establish a user in the dictionary and perform all activities cited in this finding. In addition, we found that at least two applications did not rely on the Program's "security architecture."

ACCESS CONTROLS

F. Commercial Off-the-Shelf Software Access Controls

Condition: Commercial off-the-shelf software access controls were not implemented to safeguard against unauthorized access to the mainframe computer, personal computers, and servers. Specifically, we found that:

- Resource Access Control Facility (RACF)[3] provides the capability to set rules for passwords in which the installation can require the use of specific characters (a mix of letters and numbers) within the passwords, but this feature was not used.

- A default security setting was found on a server file that allows passwords to be unencrypted.

- The "SECURE CONSOLE" command was not found on a server file which removes the Disk Operating System (DOS) from the server memory. The removal of DOS from the server memory prevents an individual from inserting a diskette into the server drive and loading unauthorized software that could perform such functions as change passwords, establish trustee rights, create users, and assign security levels. Also, the "SECURE CONSOLE" command disables the users' ability to change the server date and time, thus allowing users to bypass access restrictions.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Department's "Automated Information Systems Security Handbook" states that proprietary, personnel, sensitive, and mission-critical information should be protected from unauthorized disclosure. In addition, the Program's Automated Information Systems Security Manual states that a mix of letters and numbers is recommended for passwords used to access the Program's automated information system.

Cause: The Program's policy recommended rather than required the use of a mix of both letters and numbers in passwords to access its automated information

[3] Resource Access Control Facility (RACF) is an IBM-licensed software security product that protects information by controlling access to the information. RACF provides security by identifying and verifying users to the system, authorizing users' access to protected resources, and recording and reporting access attempts. (Resource Access Control Facility General Users Guide, Version 1, Release 9.2, 9th edition, IBM Corp., 1993, page 1-1.)

ACCESS CONTROLS

system. In addition, there was no centralized security administration for the local area networks and personal computers that contain proprietary and financial data, and no Program procedures were in place to ensure that controls were adequate to safeguard these local area networks and personal computers.

Effect: As a result, there was an increased risk that unauthorized access could be gained to the automated information system, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Evaluate the current Program policy which only recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.

2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with both recommendations. However, the Service needs to provide additional information for Recommendations 1 and 2 (see Appendix 3).

ACCESS CONTROLS

G. Access Levels Granted

Condition: We found that controls were not adequate to ensure that access levels granted to users of the Program's automated information system were appropriate. Specifically, access managers had not approved all automated information system access granted to users of the access managers' applications and had not performed periodic reviews to determine who the users were and whether the levels of access granted in the automated information system were the access levels approved.

Criteria: The "RMP Automated Information Systems Security Manual" states that supervisors and managers are responsible for ensuring that employees' ADP access certifications are appropriate for the job they will perform before users are set up to access the automated information system. Also, the "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, states: "It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date."

Cause: Program management had not ensured that its policies were implemented effectively because access managers were not included in the process of approving access to the automated information system. Additionally, the Program's policies and procedures did not require that access managers perform periodic reviews of users' levels of access to application files and system records. In addition, Program management could not efficiently, through automated means, perform reconciliations of authorization forms and access levels granted in the automated information system because the audit tools available for the automated information system had not been acquired. Although automated capabilities were not acquired, Program management could ensure that user access levels were appropriate to the work performed through a recertification process whereby users resubmit the ADP access certifications annually.

Effect: As a result, there was an increased risk that unauthorized access, data manipulation, or disclosure of proprietary information may occur. In addition, a periodic review of access files may limit the damage resulting from accidents, errors, or unauthorized use of automated information system resources and increase assurance that access levels were revised when users were reassigned or promoted or they terminated their employment. Additionally, since periodic reviews were not performed, there was an increased risk that unauthorized access would not be detected or detected timely.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.

2. Document procedures which require that users' access levels be reviewed periodically or that employees be recertified to ensure that the levels of access granted are appropriate for the duties assigned to the users.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its responses to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that it believes that "effective controls have been in place to assure that application managers approve all access to their applications." It further stated that it "acknowledge[d] that our filing system for such approvals needed improvement and are in the process of resolving this problem."

Office of Inspector General Reply. We disagree that effective controls were in place which ensured that application managers approved all access to their applications. We found that the Program did not enforce its policy which required application managers to approve all access granted to users of their applications. We performed a statistical test of users who had access to Program applications and production data and found that over 10 percent of those users tested did not have their access approved by the application manager or the Installation Security Officer. We discussed access approvals with application managers and found that these managers were unaware of how many of the users had access to the managers' applications. Therefore, the problem was not attributable to the "filing system" but to the lack of enforcement of Program policy.

ACCESS CONTROLS

Recommendation 2. Concurrence.

Service Response. The Service stated that it "concur[red] with the need to document these procedures" but "disagree[d] with the OIG's [Office of Inspector General] implication (in its statement of effect) of any significant risk of security breaches." The Service further stated: "Access to mission-critical systems has been carefully managed and controlled through documented security procedures and controls, including mainframe access matrices and annual reviews by the Security Manager. Our own tests confirmed that no unauthorized access exists or has existed."

Office of Inspector General Reply. The Service agreed that procedures should be documented but stated that it had procedures and controls in place for mission-critical systems. However, we disagree that adequate procedures and controls were in place because the Program's procedures did not address periodic reviews of users' access levels. The Service disagreed that any significant risk of security breaches would occur because mission critical systems are "carefully managed and controlled" through "documented security procedures and controls." Since the Service stated in its response to Recommendation M.1 that it had not identified all mission critical systems, it is unclear how the Service managed and controlled its mission critical systems. Regarding the annual review, under the current version of the security software, a review of user access levels within the system could not be performed. Therefore, the Program's procedures did not ensure that all users' access levels were reviewed periodically and that the levels of access granted were appropriate for the duties assigned to the users, thus ensuring implementation of "least privilege." Further, the use of the matrix identified users within a group and the group's levels of access, but it did not identify access levels for each user. In addition, without familiarity with the methodology employed in the Service's test, such as the sample selection and test performance, we must rely on the tests performed using statistical sampling software and generally accepted Government auditing standards followed by the audit staff.

ACCESS CONTROLS

H. Number of Log-in Attempts

Condition: The Program's number of unsuccessful log-in attempts to access its automated information system exceeded the standard established by the Department. Specifically, in 1992, Program management increased the number of unsuccessful log-in attempts from three to five before a user's ID and password were revoked.

Criteria: The Department's "Automated Information Systems Security Handbook" states that the number of unsuccessful log-in attempts should be three.

Cause: Program management did not follow the Departmental standard because, they stated, it was difficult for some state and tribal organizations, which are external customers, to access the mainframe computer through telephone lines.

Effect: As a result, the increased number of invalid attempts reduced the effectiveness of the password as an access control. Thus, there was an increased risk of unauthorized access to sensitive information.

Recommendation:

We recommend that the Director, Minerals Management Service, evaluate the need to deviate from the Departmental standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we consider this recommendation resolved and implemented (see Appendix 3).

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

I. Client/Server Application Software Changes

Condition: Change management controls over client/server application software were not adequate. Specifically, we found that there were no controls to ensure that: (1) Program management authorized and approved software changes and (2) the changes to the application software were adequately tested before the changed software was moved into production.

Criteria: National Institute of Standards and Technology Special Publication 500-161, "Software Configuration Management: An Overview," states that software configuration control management procedures should define the specific steps taken to analyze and evaluate the change request, clarify the meaning of the request, and resolve the problem described. In addition, the procedures should identify the appropriate individuals or organization responsible for evaluating the requests and discuss the submission of the evaluation results to the appropriate review board or individuals for approval or disapproval. Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," states that testing is a critical component of software maintenance and that, as such, test procedures must be consistent and based on sound principles. Further, the Publication states that tests should examine whether the application software is "doing what it is supposed to do."

Cause: Program management did not enforce procedures for authorizing, approving, and testing client/server application software.

Effect: As a result, there was an increased risk that the most critical client/server application software changes were not made and that applications would not perform as intended.

Recommendation:

We recommend that the Director, Minerals Management Service, enforce its procedures for authorizing, approving, and testing client server application software before the software is moved into production.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service stated that the documented procedures "are already in place."

Although the Service provided additional information in its response showing that client/server software development and change management procedures had been in place since 1995, the information, which we requested, was not provided during our audit. Based on the subsequent information provided by the Service, we agree that the Service has documented procedures. However, we found that these procedures had not been enforced during fiscal year 1997. Specifically, in our review of four client/server applications, we found no evidence to support that software changes were authorized, approved, and tested. Therefore, we have revised this finding and recommendation and request that the Service respond to the revised recommendation (see Appendix 3).

SEPARATION OF DUTIES

J. Duties Related to Client/Server Applications

Condition: The duties related to client/server applications were not separated effectively. Specifically, we found that:

- Application programmers were authorized to access client/server production data to perform "ongoing maintenance" on applications.

- At least one application programmer acted as a backup to an end user, which required the programmer to change production data in the Minerals Management Service Appeals Tracking System.

- The individual responsible for setting up users of the Royalty Management Program Desktop applications was also the person designated to review server security logs, which record the activities of the users of the applications.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that security controls for personnel include least privilege and separation of duties. The Circular states, "Least privilege is a practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job." Separation of duties is the practice of dividing the steps in a critical function among different individuals. Also, the NIST Handbook states, "Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process." The "RMP Automated Information Systems Security Manual" states, "Access to sensitive data is limited to those persons who use or process the data in performing their official duties."

Cause: Program management did not appropriately assign duties for application programmers to ensure that critical processes were not subverted. Specifically, programmers should not have access to production data because access to production data should be restricted to users. Also, Program management had not ensured that independent reviews of server security logs were performed periodically.

Effect: As a result, there was an increased risk that accidental or intentional unauthorized actions by programmers could threaten the integrity of the Program's data and disrupt system processing. Furthermore, there was an increased risk that inappropriate actions by the individuals who established system users would not be detected or would not be detected timely.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.

2. Improve detection controls by ensuring that management or the Installation Security Officer reviews server security logs periodically.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendation 2 and that it reconsider its response to Recommendation 1, which is unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated: "While application programmers do not routinely require update access to any RMP [Royalty Management Program] production data, there are instances when temporary access is needed by specific programmers under controlled circumstances. To mitigate any future risks associated with this access, procedures have been reinforced which detail actions to be taken when requesting temporary access to mainframe and client/server production data." The Service also "refute[d]" our statement that application programmers serve as backups to end users.

Office of Inspector General Reply. The Service indicated that procedures were in place to control the risk when application programmers had update access to Program data. However, we did not find such procedures; therefore, we could not test the procedures to ensure that temporary access was provided to specific programmers under controlled circumstances. To resolve this recommendation, the Service is requested to provide documentation of the procedures the Program uses that mitigate risk when programmers are allowed update access to production data.

SEPARATION OF DUTIES

Regarding application programmers serving as backups to end users, we found during our audit that a programmer analyst had been given access to a client/server application to change the database, to make table updates, and to print reports. According to Program personnel who were responsible for the application, this access was authorized so that the programmer could provide backup duties to a Program employee.

Recommendation 2. Concurrence.

Service Response. The Service stated that the contractor was "being directed to address the review of server security logs within their overall internal control procedures."

Office of Inspector General Reply. We accept the Service's alternative of having the contractor review the logs rather than Program management or the Installation Security Officer. However, regardless of who does the review, the procedures must ensure adequate separation of duties between the key functions of the security log reviewer and the security administrator.

SYSTEM SOFTWARE CONTROLS

K. Security Software

Condition: The version of RACF, the commercial mainframe security software, that was used by the Program was no longer supported by the vendor. Although the upgraded version of RACF had been purchased, it had not been implemented.

Criteria: Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," states that "the goal of software maintenance management is to keep systems functioning."

Cause: Program management had not implemented the upgraded version of RACF because management was in the process of requesting a waiver from the Department from consolidating its mainframe operations with another mainframe operation, which has the upgraded RACF, as required by Office of Management and Budget Bulletin 96-02, "Consolidation of Agency Data Centers." If the waiver is granted to the Program, the upgraded version of RACF will need to be implemented immediately.

Effect: Using security software that was not supported by the vendor increased the risk that security software would not be maintained and that programs and data files would not be protected from unauthorized access.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that the upgraded version of RACF is implemented immediately if the Program is granted a waiver from consolidating its mainframe operations with another mainframe operation.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service stated that it believes that we "misunderstood the effects of delaying this software upgrade. Although this is a moot point now that MMS [Minerals Management Service] has replaced its processor, the decision not to upgrade the RACF software was well founded."

Although the Service indicated that it had replaced its processor, we were not provided information to determine whether the Service has ensured that the upgraded version of RACF or equivalent security software was implemented on the new processor. Therefore, we

SYSTEM SOFTWARE CONTROLS

consider this recommendation unresolved and request that the Service reconsider its response to the recommendation (see Appendix 3).

Additional Comments on Finding

The Service stated that the Program "initially delayed the upgrade because it was considering a processor replacement that would require an entire new suite of mainframe software products." The Service further stated, "Upgrading RACF at that time would have been an inherently risky and potentially expensive decision." Regarding these statements, we were not provided any documentation to support these statements that the decision to not implement the upgraded version of RACF was based on the Service's plan to implement a new processor or that the upgrade of RACF would be "risky and potentially expensive."

SYSTEM SOFTWARE CONTROLS

L. Mainframe Computer System Audit Tools

Condition: Program management did not use available system audit tools to ensure integrity over system processing and data and to detect inappropriate actions by authorized users. Specifically, we found that:

- System integrity verification and audit software was not used. This software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures such as setting system options inappropriately, installing "back doors" to the operating system, and introducing viruses and Trojan horses, that can destroy production dependability and circumvent existing security measures.

- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. Additionally, system options that produce a system audit trail were not implemented. Therefore, an audit trail that logs the results of actions taken by computer operators and system programmers in the SYSLOG during system initialization could not be produced for periodic review.

- Periodic reviews of System Management Facility (SMF) logs to identify critical events affecting system processing were not performed.[4] For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as "SET TIME," "SET DATE," and "SET SMF," all of which affect system processing and production of audit trails.

- Periodic reviews of SMF logs to identify unauthorized changes to data by authorized users were not performed. Even though one of the SMF record types, record type 60, which logs all activity affecting Virtual Storage Access Method data sets that contain lease and site security data, was activated during our audit, the logs were not reviewed to detect inappropriate actions or unusual activity by authorized users.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In

[4] The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identification of users who performed the activity.

SYSTEM SOFTWARE CONTROLS

addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability is reviewing or looking at patterns of users' behavior, which requires reviews of the audit trails. The NIST Handbook states that audit trails are a technical mechanism to achieve individual accountability.

Cause: Program management did not acquire system integrity and verification software, did not implement system options to record actions taken affecting system initialization, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of resultant logs because the logs were extensive and difficult to read. Further, Program management had not considered converting the logs to a more useful format to extract critical information. Instead, Program management relied on its staff to make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect: As a result, inappropriate mainframe computer system initialization and processing were not recorded and identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or would not be detected timely and that the individual responsible would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Minerals Management Service:

1. Evaluate acquiring system verification and auditing software.

2. Implement the system options to record activities in the SYSLOG during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.

3. Evaluate the available SMF record types and implement procedures to ensure that critical SMF logs are reviewed periodically and that Program management addresses the problems identified.

SYSTEM SOFTWARE CONTROLS

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with Recommendations 2 and 3. However, the Service needs to provide additional information for Recommendations 2 and 3 and needs to reconsider its response to Recommendation 1, which is unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that the Program "routinely uses a number of system-assurance mechanisms such as control reports, system-assurance programs and user-reconciliation reports" but that it "remains alert to any technologic developments that would improve system integrity and operations." The Service further stated, "As these packages become available, they will be examined for applicability to the RMP [Royalty Management Program] computing environment."

Office of Inspector General Reply. The mechanisms cited by the Service provide information related mainly to application processing system assurance. Although the Service said that it will evaluate the use of software packages to assist in providing assurance over system integrity and operations, the Service should state concurrence or nonconcurrence with the recommendation to evaluate the acquisition of operating system-verification and auditing software that would identify mainframe operating system security exposures.

SERVICE CONTINUITY

M. Disaster Recovery Plans

Condition: Local area networks and personal computers used by the Program's divisions that maintain proprietary and financial data were not included in the Program's disaster recovery plans.

Criteria: Office of Management and Budget Circular A-130, Appendix III, states that agencies should establish a contingency plan and periodically test the plan to ensure that operations will continue in the event that automated systems fail.

Cause: Program management did not ensure that all systems which maintain proprietary and financial data were included in its disaster recovery plans.

Effect: If the disaster recovery plans are incomplete because all sensitive systems are not included, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or a system failure.

Recommendation:

We recommend that the Director, Minerals Management Service, update the disaster recovery plans to include all mission-critical systems.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for the recommendation (see Appendix 3).

Additional Comments on Finding

The Service stated, "We believe the disaster recovery plans we have in place for our mainframe and client servers provide coverage for virtually all of our mission-critical applications." In our opinion, this statement implies that disaster recovery plans are not required for other components of the Program's automated information system, such as local area networks and personal computers used by the Program's divisions. The local area networks and personal computers used by the Program's divisions were the components of the automated information system used to develop the Program's financial statements and to report financial information to the U.S. Treasury and the Office of Management and Budget. Further, these components also support the Program's mission to accurately and timely disburse rents, bonuses, and royalty revenues to the U.S. Treasury, the states, and the Indian tribes. Therefore, we believe that these components not only are "mission critical" to the Program but also are part of the Program's general support system. Office of Management and Budget Circular A-130, Appendix III, defines general support systems as "an interconnected set of information resources under the same direct management control which shares common functionality." Further, the Circular addresses the need for continuity of support for general support systems as well as major applications.

United States Department of the Interior

MINERALS MANAGEMENT SERVICE
Washington, DC 20240

JAN 16 1998

Memorandum

To: Assistant Inspector General for Audits

Through: Bob Armstrong Sylvia V. Baca JAN 21 1998
Assistant Secretary for Land and Minerals Management

From: Cynthia Quarterman Walter D. Cruickshank
Acting Director, Minerals Management Service

Subject: Office of Inspector General Draft Audit Report A-IN-MMS-001-97, "General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service"

Thank you for the opportunity to respond to this draft report on the general controls over our royalty automated information system. Of the 24 Recommendations, we agree with 11, partially agree with 2, and disagree with 11. We're sending you our general comments on the audit findings and specific ones on the recommendations. We've also included nine Enclosures to our response as additional background material for your review.

Please contact Bettine Montgomery at (202) 208-3976 if you have any further questions.

Attachments

[ENCLOSURES REFERRED TO IN THE MINERALS MANAGEMENT SERVICES' RESPONSE NOT INCLUDED BY THE OFFICE OF INSPECTOR GENERAL.]

MINERALS MANAGEMENT SERVICE RESPONSE TO DRAFT AUDIT REPORT "GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE"

Audit Agency: Office of Inspector General (OIG)

Audit Number: A-IN-MMS-001-97

We appreciate the opportunity to comment on this draft report. MMS shares OIG's concern for security and controls and concurs with some of the findings and recommendations presented in the report. In fact, the Royalty Management Program (RMP) is actively implementing solutions to rectify some of the weaknesses pointed out by the OIG and to enhance system security. We concur with OIG's use of OMB Circular A-130 as the principal criteria for evaluation; however, we cannot agree with OIG's implicit conclusion that RMP systems do not comply with the Circular. It is important to recognize these criteria are general, leaving considerable room for judgement and interpretation based on the individual facts and circumstances.

We indeed believe RMP systems are in substantial compliance with the spirit and intent of the OMB Circular and strenuously disagree with the overall conclusion of the report -- that general controls were inadequate. The OIG review identified some spot failures and procedural weaknesses, many of which we have agreed to change. However, in terms of materiality, the sum total of these weaknesses, in our opinion, is not significant enough to constitute an overall finding of inadequate. Furthermore, the report does not actually deal with the overall or general controls. To do so would require an evaluation of redundant and compensating controls. Yet, the OIG report stated "we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information system general controls."

MMS would also point out that our recurring management control reviews have addressed such manual controls and generally found they were working effectively or prompted corrective actions to resolve minor control deficiencies. While these reports, as well as the supporting workpapers, were reviewed during this and prior OIG audits of our automated system, no adverse findings in this regard were reported. Moreover, past OIG audits performed under the Chief Financial Officers Act of 1990 have covered these controls, and each report concluded that our financial information was reliable.

We must dispute many of the OIG's facts, conclusions, and interpretations. System security is a complex network of redundant measures and policies which must strike an appropriate balance between risk and cost. Taken together, this network provides overall security for the key operating systems. No system is perfect, especially given the rapidly changing technological environment and the competing needs for funds. However, we believe OIG is holding RMP to an unattainable standard in concluding general controls were "not adequate." MMS has established and continues to improve on a system of security controls that we believe should instead be viewed as a positive example, or even a model within the government.

Finally, the OIG report does not demonstrate a single negative impact of its findings. The OIG reported no incidents -- no loss or corruption of data and no theft or unauthorized access. We believe the absence of such incidents reflects favorably on our existing automated and manual compensating controls. Our primary comments on the facts and conclusions are shown below by topic. Additional comments on the facts and conclusions are included in our comments on the recommendations.

RISK ASSESSMENTS

MMS believes the risk assessment criteria were not appropriately applied. Circular A-130 states *"The Appendix no longer requires the preparation of formal risk analyses"* and that risk assessments *"can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments."* Given the breadth of judgement allowed on this matter, RMP's previous risk assessment documents and processes were clearly in accordance with the guidelines. We must also disagree with OIG's findings that MMS did not properly assess the risks regarding year 2000 program conversion, "unsupported" system security software, and "geopolitical" and "external directives" risks.

In 1996, RMP management anticipated the potential risks associated with the Year 2000 conversion and tasked its operations and maintenance contractor to conduct a detailed analysis of major systems and develop a plan for modifying and testing the programs. The resultant $1.6 million project was begun by the contractor in March 1997 and is on track for completion in 1998. (Enclosures 1, 2, 3 and 4). In May 1997, RMP management also initiated a parallel internal project to assess non-mainframe, stand-alone systems. Given the fact that OMB Circular A-130 does not even require formal risk analyses; it would seem that such an explicit recognition of this risk and timely action toward its elimination is as an accomplishment rather than a failure.

We also believe the OIG misunderstood the circumstances involving the "Resource Access Control Facility" (RACF) mainframe security software. The system-security software was never "unsupported" in the sense implied by OIG; this was a contractual matter that would have required a paid service call rather than a supported call if a problem arose. Because RMP was planning to upgrade to a different operating system, we chose not to incur the expense of a software upgrade at that time. RMP was never at any risk regarding this software.

We also take issue with OIG's opinion regarding our assessment of "geopolitical" and "external directives" risks. In our view, OIG's opinion that RMP was at risk of employee sabotage because of low morale associated with potential program abolishment or downsizing is overstated. Since the program's inception in 1982, RMP employees have become accustomed to such proposals. While they may indeed weaken morale, we have learned external threats are more likely to rally our employees than to foster mischief. While we consider the employee morale issue to be important matter, RMP correctly assessed this risk as "low."

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

RMP disagrees with OIG's statement that "Program management did not have procedures to ensure that client/server application software changes were authorized, approved, and tested before being moved into production." Such procedures have been in place since 1995 and are published in an on-line help text format (Enclosure 5). The Client/Server Guidelines clearly define the steps/processes for testing to be included in the Implementation Plan (part of the Visualization Step) and the Unit, System, and User Testing required as part of the Operational Prototype (Development Step). These Guidelines include a separate Procedural Overview of Testing including an example test plan. While testing processes for client-server applications are different from those for mainframe systems because of the emphasis on interactive prototyping and Graphical User Interface design, they are no less adequate.

DEFAULT SETTINGS

The OIG found one instance where a default ID provided with off-the-shelf software was not removed as required. However, it is factually incorrect to say that use of this default ID allows access to all mainframe computer resources. The security architecture prevented any unauthorized or inappropriate user from using this ID because users must first be able to access the system through a valid RACF logon password and have a user ID defined to the data dictionary. At no time were RMP resources at risk

SECURITY SOFTWARE

The OIG seems to have misunderstood the reasons for and the effects of RMP's decision not to upgrade RACF, the commercial mainframe security software. As noted above, RMP initially delayed the upgrade because it was considering a processor replacement that would require an entire new suite of mainframe software products. Upgrading RACF at that time would have been an inherently risky and potentially expensive decision. Moreover, the current version of RACF had been very stable. The only risk of running "unsupported" software is contractual; that is, in the unlikely event of a RACF failure, IBM would have to be called in for service on demand rather than as a fully supported maintenance call.

DISASTER RECOVERY PLANS

The OIG seems to have generalized two distinct concepts and used them interchangeably. Sensitive or proprietary information is not synonymous with mission critical-systems and information. Although most MMS mission-critical information is sensitive, the reverse is not the case. Most sensitive data is not mission critical.

The central repository for mission-critical information resides on the mainframe computer. This is where MMS's key systems reside--the heart of the MMS' operations--requiring a comprehensive disaster recovery plan. Users know they can always go to this central repository for the official and current data. This database is updated continuously, centrally managed, and routinely backed up. Because most of this data is also business-sensitive, security controls are also in place to prevent unauthorized disclosure.

In addition, large amounts of redundant data reside in paper and electronic format in and on desks, file cabinets, and personal computers. This includes sensitive and financial data. However, because most of this data is redundant, it is not "mission critical." Therefore, while it is important to prevent unauthorized disclosure of this information, disaster recovery plans are, in most cases, not cost effective, feasible, or necessary.

Therefore, OIG's conclusion that disaster recovery plans are needed for *all local area networks and personal computers that contain proprietary and financial data* is erroneous. We believe the disaster recovery plans we have in place for our mainframe and client servers provide coverage for virtually all of our mission-critical applications. We are currently reviewing "stand alone" PC systems to determine if any are truly mission critical. If so, they will need to be brought onto the network and managed accordingly.

COMMENTS ON RECOMMENDATIONS

A1. Ensure that risk assessments are conducted in accordance with guidelines, which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.

DISAGREE - While MMS plans to enhance and better document our risk assessment process due to the rapidly changing computing and communication environment, we believe our previous assessments were in accordance with guidelines.

A2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.

DISAGREE - RMP policies define the LAN administrators' role in contingency planning and security. (Enclosure 6).

A3. Determine the risks associated with local area network applications and personal computer databases that contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.

AGREE - RMP will conduct a risk analysis on user written applications as well as data residing on networks and personal computers to determine appropriate security and disaster recovery procedures. An inventory of these applications and the business functions they support is already being performed as part of RMP's Year 2000 project.

B1. Evaluate Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity level is greater than the position sensitivity levels of the employees who are performing the work.

PARTIALLY AGREE - We plan to reevaluate the position sensitivity level for the senior personnel in charge of the contractor activity to determine if those position should be classified at a higher level. In accordance with Departmental criteria, most ADP staff are designated noncritical sensitive. We doubt it was the OIG's intention to imply that *all* work must be reviewed by persons at a higher sensitivity level; however, this would be impossible in a multiple level organization because there are only two sensitivity levels from which to choose, i.e., "noncritical-sensitive" and "critical-sensitive."

B2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.

PARTIALLY AGREE - We agree controls are needed to assure the contractor timely submits requests for background checks. The contractor has been directed and has begun to track and is accountable for the status of its submission of these requests. We also agree that employees awaiting clearances should be in probationary status; however, it would be unacceptably costly to prohibit employees from performing critical ADP work. Except for positions which require access to information dealing with national security, all Federal employees are hired and perform the full scope of their jobs while the appropriate investigation is conducted and a suitability determination is made. We believe a similar criterion is appropriate for our contractors. Most all software development and system operation work could be considered critical. As a practical matter, we could not delay replacing contractor employees in such work pending the completion of background checks. However, we are exploring alternatives with the contractor such as having them perform a preliminary "criminal and credit check" which is quick and inexpensive .

B3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic follow-up background checks are performed as required.

DISAGREE - Controls are already in place to ensure that personnel or security files accurately reflect background checks. MMS's Office of Administration and Budget maintains documentation and a tracking system on all MMS employee and contractor security clearances and background checks. We also disagree with the OIG's statement that followup background checks are required. MMS is in compliance with Departmental guidance (Enclosure 7) that followup checks are authorized *only* for national security positions and not for public trust positions.

C1. Establish controls to enforce Program policy that requires employees to sign security awareness statements before their access to system resources is approved by the Installation Automated Information System Security Officer.

AGREE - While our own test sample has confirmed that our users have appropriate access to RMP systems, we concur that our filing system for access approvals needed improvement. All statements are now consistently filed and reconciled by the ADP security officer.

D1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.

DISAGREE - We believe our current classifications are appropriate. Most RMP data is sensitive or "proprietary" and must be protected from unauthorized disclosure. Our mainframe systems receive heightened security because they are more mission critical, not because they are more sensitive. As explained in previous segments, these systems must be protected more strenuously to ensure the integrity of the official records.

A more moderate level of protection is necessary for proprietary information than for mission critical information. The umbrella protection mechanism for all types of proprietary information is physical controls coupled with employee training. RMP works in a secure environment and trains employees to protect all forms of proprietary information such as paper copies, information on their PC's, and floppy disks, in addition to information which resides on networks and servers. While it would be possible to install network security measures equivalent to the mainframe measures, we believe the significant additional cost would not be justified. We believe the protection level over all proprietary information is appropriate.

The OIG is technically correct in its statement that MMS had not officially designated any of its systems as "major". However, RMP has treated its mission-critical mainframe applications as major (as allowed by OMB Circular A-130) by providing extra security controls and disaster recovery capabilities. Based on our interpretation of A-130, the fact that these systems were not officially designated as major systems in our annual security plan is incidental and not substantive.

D2. Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.

DISAGREE - We believe our existing access controls over resources already meet the intent of this recommendation. All MMS employees are granted access to view royalty, production, and reference data. Since most of this data is proprietary, employees are trained in its proper use and must sign statements acknowledging their responsibility to protect it. State and Tribal employees have access to such data within their jurisdictions only. The ability to add or change data is limited to those employees who require that access to perform their jobs.

E1. Implement controls to enforce Program policy that default user ID's and passwords are to be removed from the automated information system when commercial off-the-shelf software is implemented.

AGREE - The contractor has implemented a verification procedure to ensure this situation does not recur.

F1. Evaluate the current Program policy which only recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.

AGREE - RMP will assess this issue and document the decision.

F2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.

AGREE - We are in process of implementing centralized security administration for efficiency purposes. However, we cannot support OIG's basis for this recommendation, i.e., that "... no Program procedures were in place to ensure that controls were adequate to safeguard these local area networks and personal computers" as evidenced by two allegedly inappropriate software settings. As discussed below, we disagree the settings are inappropriate. RMP has had security and recovery procedures in place for its LAN's since 1993, and the fileservers are secure.

F3. Change the "SET UNENCRYPTED PASSWORD" to "OFF" and include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining unauthorized access to sensitive files.

DISAGREE - RMP was aware of the software settings issues suggested by the OIG and had consciously decided to leave the settings as they are. In both cases, the judgements were based on operational issues, taking risk into consideration. The limited security exposure was mitigated by the physical controls. The servers in question are in a locked LAN room within a controlled access building. Both of these decisions fall under the security judgement mandated by the A-130 and the National Institute of Standards and Technology (NIST) handbook which states that "The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits". It was RMP's judgement that the real costs of setting these parameters in the way suggested by OIG clearly exceeded their limited security benefits.

G1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.

DISAGREE - We believe effective controls have been in place to assure that application managers approve all access to their applications (see Enclosure 7). We acknowledge that our filing system for such approvals needed improvement and are in the process of resolving this problem.

G2. Document procedures which require that users' access levels be reviewed periodically or that employees be re-certified to ensure that the levels of access granted are appropriate for the duties assigned to the users.

AGREE - We concur with the need to document these procedures. However, we disagree with the OIG's implication (in its statement of effect) of any significant risk of security breaches. Access to mission-critical systems has been carefully managed and controlled through documented security procedures and controls, including mainframe access matrices and annual reviews by the Security Manager. Our own tests confirmed that no unauthorized access exists or has existed.

H1. Evaluate the need to deviate from the Departmental standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.

AGREE - A DOI waiver for RMP to extend the password attempts from three to five for the RMP was granted on November 14, 1997. (Enclosure 9)

I1. Document procedures for authorizing, approving, and testing client/server application software before the software is moved into production.

DISAGREE - These documented procedures are already in place. (Enclosure 5)

J1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.

DISAGREE - While application programmers do not routinely require update access to any RMP production data, there are instances when temporary access is needed by specific programmers under controlled circumstances. To mitigate any future risks associated with this access, procedures have been reinforced which detail actions to be taken when requesting temporary access to mainframe and client/server production data. We also refute OIG's statement that application programmers serve as "backup" to end-users. This does not occur.

J2. Improve detection controls by ensuring that management or the Installation Security Officer reviews server security logs periodically.

AGREE - The contractor is being directed to address the review of server security logs within their overall internal control procedures. (We do not believe MMS management or the Installation Security Officer should carry out this procedure.)

K1. Ensure that the upgraded version of RACF is implemented immediately if the Program is granted waiver from consolidating its mainframe operations with another mainframe operation.

DISAGREE - As discussed under Risk Assessments (Page 2), we believe OIG misunderstood the effects of delaying this software upgrade. Although this is a moot point now that MMS has replaced its processor, the decision not to upgrade the RACF software was well founded.

L1. Evaluate acquiring system-verification and auditing software.

DISAGREE - RMP routinely uses a number of system-assurance mechanisms such as control reports, system-assurance programs and user-reconciliation reports. Nonetheless, RMP remains alert to any technologic developments that would improve system integrity and operations. As these packages become available, they will be examined for applicability to the RMP computing environment.

L2. Implement the system options to record activities in the SYSLOG during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.

AGREE - System initialization activities as well as operator commands are already recorded in the SYSLOG. Because we are uncertain of the payoff and cost effectiveness of the periodic reviews, we will conduct a pilot test. The SYSLOG will be reviewed following system initialization for inappropriate and unauthorized activities that may have occurred during the test. Based on the results, we will assess the feasibility of fully implementing this routine.

L3. Evaluate the available System Management Facility (SMF) record types and implement procedures to ensure that critical SMF logs are reviewed periodically and that Program management addresses the problems identified.

AGREE - We have evaluated record types and concluded that certain log record types may be worthwhile for periodic review. We will pilot test a monthly review of these record types. Depending on the volume of records and the payoff, RMP will continue, expand, or reconsider this detection method. Program management will be notified when problems are identified.

M1. Update the disaster recovery plans to include all mission-critical systems.

AGREE - We plan to update the disaster recovery plans to include all mission-critical systems. However, we do not agree with the OIG's presumption that all systems containing proprietary or financial data are "mission critical." Many PC-based systems contain *copies* of such data for analysis, but these systems are not considered mission critical. MMS' ongoing Year 2000 project is identifying and classifying any stand-alone systems that managers judge to be "mission critical." If so, these systems will be reclassified as such and will be required to reside on LAN's or servers that can be centrally backed up for recovery purposes.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1	Unresolved.	Reconsider the recommendation to clarify that the enhanced risk assessment process will include the identification of significant risks affecting systems, will appropriately identify controls implemented to mitigate those risks, and will formalize the acceptance of residual risk. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
A.2	Unresolved.	Reconsider the response to ensure that local area network administrators participate in the risk assessment process, and provide an action plan that includes target dates and titles of officials responsible for implementation.
A.3, F.1, F.2, L.2, L.3, and M.1	Management concurs; additional information needed.	Provide an action plan that includes titles of officials responsible for implementation.
B.1, B.2, E.1, and J.2	Management concurs; additional information needed.	Provide an action plan that includes target dates and titles of officials responsible for implementation.

Finding/Recommendation Reference	Status	Action Required
B.3, D.1, D.2, and L.1	Unresolved.	Reconsider the recommendations, and provide action plans that include target dates and titles of officials responsible for implementation.
C.1	Unresolved.	Provide information relating to how the reconciliation of the statements was performed and the dates the actions were completed.
G.1	Unresolved.	Reconsider the recommendation, and provide information regarding controls which ensure that all access managers approve all access to their applications. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
G.2	Unresolved.	Reconsider the recommendation, and provide information regarding documentation of procedures requiring users' access level reviews or recertification of users' access be performed periodically. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
H.1	Implemented.	No further action is required.

Finding/Recommendation Reference	Status	Action Required
I.1	Unresolved.	Respond to the revised recommendation, and provide an action plan that includes target dates and titles of officials responsible for implementation.
J.1	Unresolved.	Reconsider the recommendation, and provide the procedures that mitigate risks when application programmers are allowed update access to production data.
K.1	Unresolved.	Reconsider the recommendation, and provide information on whether the upgraded version of the security software has been implemented on the new processor.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240

Our 24-hour
Telephone HOTLINE
1-800-424-5081 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420 or
1-800-354-0996

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior
Office of Inspector General
Eastern Division - Investigations
1550 Wilson Boulevard
Suite 410
Arlington, Virginia 22209

(703) 235-9221

North Pacific Region

U.S. Department of the Interior
Office of Inspector General
North Pacific Region
238 Archbishop F.C. Flores Street
Suite 807, PDN Building
Agana, Guam 96910

(700) 550-7428 or
COMM 9-011-671-472-7279

Toll Free Numbers:
1-800-424-5081
TDD 1-800-354-0996

FTS/Commercial Numbers:
(202) 208-5300
TDD (202) 208-2420

HOTLINE

1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240